THE END OF THE SEARCH

What Cryptography Got Wrong.
And Why It Doesn't Matter Anymore.

Paul McGough · NQP LLC · April 2026 (rev. June 2026)

Shannon called it "weaker." He was measuring the wrong thing.

In 1949, Shannon proved two things. First: the One-Time Pad is perfectly secret — provably, forever, for any adversary including quantum. The key must be as long as every message, never reused. Unusable at scale.

Second: a finite, reusable-key cipher he called an Ideal System, defined precisely as permanently leaving the adversary unable to find a unique solution:

> *"no matter how much material is intercepted, the enemy still does not obtain a unique solution to the cipher but is left with many alternatives, all of reasonable probability."*

Then he called it weaker. Then he walked away.

And all of cryptography walked away with him — for 75 years.

RSA. AES. ECC. Six trillion dollars a year in cybercrime later — Hard Enough isn't looking so good.

These ciphers rely on assumptions about computational difficulty — conjectured, not proved. Some already invalidated. Others facing quantum. The security was always hard to break, not impossible to break.

And even where they hold, they are impractical. They demand dedicated hardware to run at usable speed. They struggle on constrained devices — sensors, embedded systems, the low-power hardware where the real world actually operates. Post-quantum replacements are heavier still: larger keys, greater overhead, more complexity. Every generation of Hard Enough requires more resources to stay ahead of a threat it cannot actually stop.

Hard to break. Hard to run. Impractical.

Ask Mary, Queen of Scots what happens when the technology doesn't match the requirement. She lost her head. The requirement has only ever been one thing: **Unreadable. Works everywhere. Forever.**

© 2026 NQP LLC. All rights reserved.

RPM@enqpy.com

There is only one question that matters.

Shannon's framework for measuring secrecy tracks how many wrong answers the adversary faces, and how their probability of guessing correctly changes as they observe more ciphertext. This is rigorous mathematics. It is also the wrong question.

The wrong question is: "how many alternatives face the adversary?"

The right question is: can the adversary determine the answer?

Not "how hard is the search." Not "how many wrong answers surround the right one."

Can. They. Determine. It.

For Perfect Secrecy: no. Shannon proved this in 1949.

For the Enqpy™ Ideal System — non-uniqueness proved on both independent axes: no. Proved now.

The outcome is identical. The adversary cannot determine the message in either case.

Shannon called the Ideal System "weaker" because it leaves the adversary facing fewer wrong answers than Perfect Secrecy. Fewer wrong answers is a difference in *cardinality* — the size of the uncertainty set. But cardinality only matters if the adversary can use it to eventually converge on the right answer. Enqpy's proof makes arrival permanently impossible: no quantity of ciphertext ever yields a unique solution. Under that binary question — can they determine it? — when the destination is permanently unreachable, the rate of approach toward it has no consequence.

Weaker was the wrong word. Enqpy™ proved it.

Enqpy™ is the first finite-key cipher formally proved to satisfy Shannon's Ideal System definition — derived from algebra, not computational assumptions, and unconditional for any adversary, including quantum, for any quantity of ciphertext, forever.

The adversary never learns which key was used. The adversary never determines which plaintext was sent. The uncertainty is permanent. Unlike the One-Time Pad, Enqpy™'s key is not infinite — it is finite and reusable. The cipher runs everywhere.

Unreadable and usable are not opposites. They are not in tension. They are the same requirement, and they are now both met.

© 2026 NQP LLC. All rights reserved.

RPM@enqpy.com

The hierarchy of cryptography must be reordered.

Shannon ranked Perfect Secrecy first and called the Ideal System weaker. That ranking was made before anyone had proved the Ideal System — with non-uniqueness on both axes — with a finite key. It was made in the absence of evidence. The evidence now exists.

Here is the correct order:

1. **Proved Ideal System + two-axis non-uniqueness + practical** (Fast · Efficient · Flexible · Finite key)
   ← **THIS IS WHERE WE ARE NOW**
2. **Perfect Secrecy (OTP)** — unconditional, but requires infinite key. Same adversarial outcome. Practically unusable.
3. **Computational security (AES / RSA / post-quantum)** — practical, but conditionally breakable. Expiring now.

Unreadable on Mars is worthless on Earth. The pinnacle of cryptography must be the thing that is both: provably unreadable, and usable by human beings in the real world.

That thing now exists. It has a name.

The complete set has been found.

For 75 years, cryptography searched for properties one at a time: secure, then fast, then flexible, then quantum-safe. It never found all of them at once, because it was looking for each one independently.

The search should have been for the entire SET. The entire property set that makes encryption actually work:

Fast · Efficient · Flexible · Unreadable · Proved

That set — all five properties, simultaneously, unconditionally, with a finite key — has not had a name. It should.

© 2026 NQP LLC. All rights reserved.

Absolute Secrecy.

No adversary. No platform. No algorithm. No passage of time. No exceptions.
No key. No message. Nothing is in the ciphertext. The math proves it.

"Perfect" Secrecy requires an infinite key. "Absolute" Secrecy requires only a finite one — and delivers the same outcome to the adversary. The distinction matters: *Perfect* Secrecy was named for its mathematical elegance. *Absolute* Secrecy is named for its real-world result. The adversary never determines the message. Not eventually — never. Not with more computing power — never. Not with a quantum computer — never. The key is finite. The cipher runs on any device. The security is permanent.

The search is over. The property set is complete. The proof exists. The implementation runs.

To the people of the world:

You have been kept secure by mathematics that is hard to break, not impossible to break. Every breach where the cipher was the failure happened because the security was imperfect, not absolute.

The thing you actually needed — provably unreadable security that runs on any device, for any message, with a key you can keep forever — has existed in Shannon's equations since 1949. Nobody built it. Nobody proved it.

Somebody did now.

Gilbert Vernam built the cipher. Claude Shannon proved the theory. Paul McGough proved the practice.

This is the end of the cryptographic search that began the moment human beings first tried to send a secret. The question is answered. The proof is filed. The implementation ships.

Enqpy™ · Security, Settled. · Proved. Not assumed.

NQP LLC · Paul McGough · RPM@enqpy.com · April 2026 (rev. June 2026)

© 2026 NQP LLC. All rights reserved.

"Major advances in science do not result from small, incremental steps but instead from sudden and occasional sea changes, 'paradigm shifts,' in which a completely new view is proposed and finally accepted by the community of scientists."

— Thomas Kuhn, The Structure of Scientific Revolutions (1962)

"All truth passes through three stages. First, it is ridiculed. Second, it is violently opposed. Third, it is accepted as being self-evident."

— attributed to Arthur Schopenhauer

© 2026 NQP LLC. All rights reserved. RPM@enqpy.com